Memo of Meeting

Date: April 19, 2002
Location: 1350 Piccard Drive, Rockville, Maryland 20850

Representing Vector Intelligence, Inc.
2200 Benjamin Franklin Parkway, Suite 514-South
Philadelphia, PA 19130

John C. Gregory, Interim CEO
Eric Rugart, Acting Chief Technology Officer

Representing FDA:

Charles Snipes, Compliance Officer, Center for Drug Evaluation and Research
Allen Wynn, Consumer Safety Officer, (detailed to Office of Enforcement from) Center For Devices and Radiological Health
Scott MacIntire, Director, Division of Compliance Information and Quality Assurance, Office of Enforcement
Tom Chin, Consumer Safety Officer, Office of Enforcement
Paul J. Motise, Consumer Safety Officer, Office of Enforcement

The meeting was held at the request of the Vector Intelligence representatives, to discuss their biometric based electronic signature software, BioSig™, in the context of 21 CFR Part 11. The firm promotes its product as enabling their users to meet requirements of part 11 and the Health Insurance Portability and Accountability Act. At the start of the meeting we explained that FDA does not formally review, approve or disapprove of products or services that enable people to comply with FDA regulations. We advised that the meeting would be an information exchange and that our comments should not be taken as formal FDA positions.

At the start of the meeting we also asked the representatives to tell us if they considered any information, including the contents of several publications they gave us, to be confidential, trade secret or otherwise of a nature that they would not want included in a publicly available memo of our meeting. The publications are attached.

The Vector Intelligence representatives explained that their company produces biometric electronic signature software that is intended to be used with digitizers that can provide x,y, and t coordinates where x and y are positions on the digitizer and t is time. The software measures 23 biometric vectors (parameters) including speed, stroke direction, and order associated with writing one’s signature. The representatives explained that their software is capable of measuring stylus pressure, as well, but that this feature is disabled due to background “noise”. The software uses technology developed by Bell Labs and patented by Lucent Technologies. The software is portable to Windows CE devices, the E-Pad and other PC based pad devices, but not to Palm platform devices.

The representatives explained that they developed their product primarily for use by healthcare/pharmacy companies that track drug samples.

During the meeting we discussed the firm’s validation efforts. The representatives said they would welcome customer audits of their software development activities. The firm will also provide software functional specifications and test scripts.

During the meeting we discussed the system’s false acceptance and false rejection rates. The representatives explained that the system has an error rate of about 1.2%. The software permits system administrators, but not end users, to configure and adjust the system’s sensitivity on a scale of 1 to 6 and the system accuracy on a scale of 1 to 200.

Biometric templates, against which a person’s signing action would be compared for authentication purposes, reside on either a remote server or the local computer. The representatives said they anticipated expanding to the use of smart cards that would hold the user’s template. The template takes 100 bytes of storage without a graphical image and 3K to 5K of storage with a graphical image of the signature.

We asked if the system was designed to adjust to changes in the biometric traits that may occur over time. We commented that such a feature was not a requirement of part 11 but that we had seen some systems that automatically adjusted to such changes. The representatives said that the system does not make such automatic changes and that over a period of time end users may need to be re-enrolled to account for the natural changes in how they execute a handwritten signature.

The representatives also explained that the system does not have a back-up identification code/password feature, (e.g., should an end user be injured or otherwise unable to execute a manual signature).

With respect to the manifestation of the biometric electronic signature, the representatives explained that the system displays the user’s printed name, date and time of signing and the purpose of the signature.

The meeting lasted about two hours.

cc:
FDA Attendees
HFA-224
Part 11 Guidance Dockets

Doc ID VectorIntelligenceMemoOfMeeting041902.doc
P. Motise 05/15/02